

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-241989

(43)Date of publication of application : 29.08.2003

(51)Int.Cl.

G06F 11/00

G06F 15/00

(21)Application number : 2002-039087

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 15.02.2002

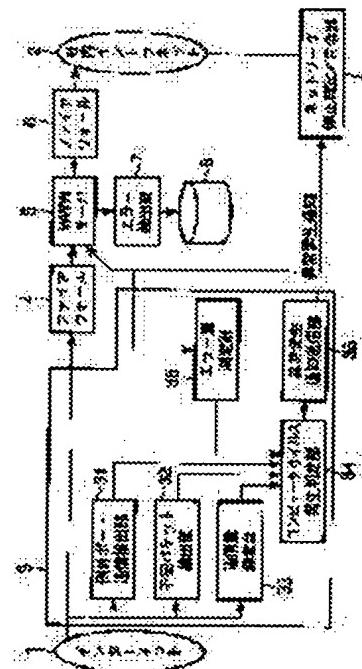
(72)Inventor : TAKAHASHI TOSHINARI

(54) COMPUTER VIRUS OCCURRENCE DETECTING DEVICE, METHOD AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a computer virus occurrence detecting device, method and program capable of early detecting occurrence of computer virus on a network to prevent the infection damage by computer virus on a computer network or computer system that is an object of security protection.

SOLUTION: This computer virus occurrence detecting device 3 early detects whether a computer virus has occurred on Internet 1 or not as the computer virus remains unspecified. Namely, the occurrence of computer virus is detected in a state before the kind or mechanism is clarified and countermeasure data such as vaccine is provided, or an unknown computer virus state. For such a detection, this device is constituted to collect specific data showing the probability of occurrence of computer virus. The specific data is formed of data showing the occurrence of imperfect packet, abnormal increase in communication quantity, abnormal increase in error quantity, or the like, which is caused by a TCP/IP communication using an exceptional port generally not used or an abnormal TCP/IP communication.



LEGAL STATUS

[Date of request for examination] 17.04.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

[decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-241989

(P2003-241989A)

(43)公開日 平成15年8月29日(2003.8.29)

(51)Int.Cl.⁷
G 0 6 F 11/00
15/00

識別記号
3 3 0

F I
G 0 6 F 15/00
9/06

テーマコード(参考)
3 3 0 A 5 B 0 7 6
6 6 0 N 5 B 0 8 5

審査請求 有 請求項の数12 O L (全 9 頁)

(21)出願番号 特願2002-39087(P2002-39087)

(22)出願日 平成14年2月15日(2002.2.15)

(71)出願人 000003078
株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 高橋 傑成
神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

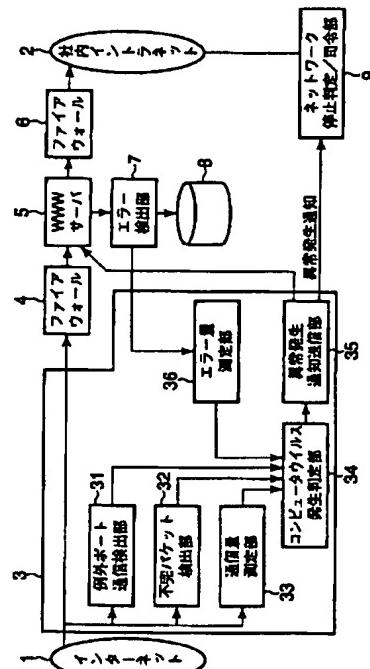
(74)代理人 100058479
弁理士 鈴江 武彦 (外6名)
Fターム(参考) 5B076 FD08
5B085 AC14 AE00 BG07

(54)【発明の名称】 コンピュータウイルス発生検出装置、方法、およびプログラム

(57)【要約】

【課題】ネットワーク上でのコンピュータウイルスの発生を早期に検出し、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムへのコンピュータウイルスの感染被害を未然に防止できるコンピュータウイルス発生検出装置、方法、およびプログラムを提供すること。

【解決手段】コンピュータウイルス発生検出装置3はインターネット1上にコンピュータウイルスが発生したか否かを、同コンピュータウイルスを不特定のまま早期に検出する。すなわち、種別やその仕組み等が明らかとなつてワクチン等の対策データが提供される以前の状態、つまり未知コンピュータウイルスの状態でその発生を検出する。かかる検出のために、コンピュータウイルスの発生の可能性を示す特異データを収集するよう構成される。特異データとは、通常は使用されない例外ポートを使用したTCP/IP通信が行われたこと、異常なTCP/IP通信が行われたことによる不完全なパケットの発生、通信量の異常な増加、エラー量の異常な増加等を示すデータから構成される。



【特許請求の範囲】

【請求項1】 コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集手段と、

前記収集手段により収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定手段と、を具備することを特徴とするコンピュータウイルス発生検出装置。

【請求項2】 前記収集手段は、通常は使用しないポートを指定したネットワーク通信の発生有無を、前記特異データとして検出する例外ポート通信検出手段を具備することを特徴とする請求項1に記載のコンピュータウイルス発生検出装置。

【請求項3】 前記収集手段は、所定の通信プロトコルに従うパケット通信処理における通常とは異なる処理の発生を前記特異データとして検出する例外ポート通信検出手段を具備することを特徴とする請求項1に記載のコンピュータウイルス発生検出装置。

【請求項4】 前記収集手段は、前記コンピュータネットワークにおける通信量の異常増加を前記特異データとして検出する通信量測定手段を具備することを特徴とする請求項1に記載のコンピュータウイルス発生検出装置。

【請求項5】 コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置に付帯のコンピュータウイルス発生検出装置であって、前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集手段と、

前記収集手段により収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定手段と、

前記コンピュータウイルス発生判定手段により判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知手段と、を具備することを特徴とするコンピュータウイルス発生検出装置。

【請求項6】 前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムは、前記通知手段による通知を受けて前記コンピュータウイルスが発生し得るコンピュータネットワークとの接続を遮断する手段を具備することを特徴とする請求項5に記載のコンピュータウイルス発生検出装置。

【請求項7】 前記コンピュータウイルス発生判定手段により判定されたコンピュータウイルスを駆除する駆除手段をさらに具備することを特徴とする請求項5又は6に記載のコンピュータウイルス発生検出装置。

【請求項8】 前記収集手段は、ネットワークアクセス

10

20

30

40

50

において生じたエラー量の異常増加を前記特異データとして測定するエラー量測定手段を具備することを特徴とする請求項5に記載のコンピュータウイルス発生検出装置。

【請求項9】 コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、

前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、を具備することを特徴とするコンピュータウイルス発生検出方法。

【請求項10】 コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置におけるコンピュータウイルスの発生を検出するコンピュータウイルス発生検出方法であって、

前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、

前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、

前記コンピュータウイルス発生判定ステップにおいて判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知ステップと、を具備することを特徴とするコンピュータウイルス発生検出方法。

【請求項11】 コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、

前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、をコンピュータに実行させるコンピュータウイルス発生検出プログラム。

【請求項12】 コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置におけるコンピュータウイルスの発生を検出するウイルス発生検出プログラムであって、

前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、

前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生検出判定ステップと、

前記コンピュータウイルス発生判定ステップにおいて判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知ステップと、をコンピュータに実行させるコンピュータウイルス発生検出プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンピュータシステムのセキュリティに関し、コンピュータネットワーク上におけるコンピュータウイルスの発生を早期に検出するコンピュータウイルス検出装置、方法、およびプログラムに関する。

【0002】

【従来の技術】近年、コンピュータシステムあるいは個々のハードウェアやソフトウェアを、災害や故障、不正な侵入やコンピュータウイルスなどによる破壊、改変から守るためにセキュリティ技術が注目を集めている。特に、インターネットやイントラネットの急速な普及に応じて、ネットワーク上でのセキュリティが重要視されている。

【0003】従来、コンピュータウイルスの混入を防ぐためには、例えばトレンドマイクロ社提供のウイルスバスター等のいわゆるフィルタリングソフトを利用した対策を講じるのが主流である。このフィルタリングソフトでは、ワクチンなどと呼ばれる対策データによりコンピュータウイルスを検出し、これを駆除するようにしている。

【0004】また、マイクロソフト社のWindows(R)といったオペレーティングシステム(OS)のセキュリティホールについて被害をもたらす類のコンピュータウイルスに対しては、セキュリティホールを埋めるよう手当する修正プログラムを適用し、コンピュータウイルスの被害を防止することも行われている。

【0005】しかしながら、これら従来のコンピュータウイルス対策はいずれもコンピュータウイルスが発見、特定された後に行われる所以あり、新しい(未知の)コンピュータウイルス被害に対して常に後手に回るものである。これは、コンピュータウイルスの発生からその対策までの期間に相当するタイムラグが生じることを意味する。このため、ワクチンや修正プログラムなどの対策データが配布される前の数時間に急速にコンピュータウイルスが蔓延し、多大な被害をもたらすという問題がある。

【0006】

【発明が解決しようとする課題】いわゆる社内ネットワークなど、ファイアウォールを備えたイントラネット内部へのコンピュータウイルス感染はコンピュータウイルスを含んだ電子メールの受信や、社外ホームページへのアクセスなどといった人間系を起点として発生する。こ

のため、インターネット上のコンピュータウイルス発生よりも1~10時間程遅れを生じるのが普通である。また、ほとんどのコンピュータウイルスはhttpなどのTCP/IP通信を通じて他のコンピュータシステムに順次感染するとされている。

【0007】本発明はかかる事情を考慮してなされたものであり、ネットワーク上のコンピュータウイルスの発生を早期に検出し、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムへのコンピュータウイルスの感染被害を未然に防止できるコンピュータウイルス発生検出装置、方法、およびプログラムを提供することを目的とする。

【0008】

【課題を解決するための手段】本発明に係る第1のコンピュータウイルス発生検出装置は、コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集手段と、前記収集手段により収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定手段と、を具備することを特徴とするコンピュータウイルス発生検出装置である。

【0009】本発明に係る第2のコンピュータウイルス発生検出装置は、コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置に付帯のコンピュータウイルス発生検出装置であって、前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集手段と、前記収集手段により収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定手段と、前記コンピュータウイルス発生判定手段により判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知手段と、を具備することを特徴とするコンピュータウイルス発生検出装置である。

【0010】本発明に係る第1のコンピュータウイルス発生検出方法は、コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、を具備することを特徴とするコンピュータウイルス発生検出方法である。

【0011】本発明に係る第2のコンピュータウイルス発生検出方法は、コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置におけるコンピュータ

ウイルスの発生を検出するコンピュータウイルス発生検出方法であって、前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、前記コンピュータウイルス発生判定ステップにおいて判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知ステップと、を具備することを特徴とするコンピュータウイルス発生検出方法である。

【0012】本発明に係る第1のコンピュータウイルス発生検出プログラムは、コンピュータネットワーク上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、をコンピュータに実行させるコンピュータウイルス発生検出プログラムである。

【0013】本発明に係る第2のコンピュータウイルス発生検出プログラムは、コンピュータウイルスが発生し得るコンピュータネットワークと、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムとの間に接続されるサーバ装置におけるコンピュータウイルスの発生を検出するウイルス発生検出プログラムであって、前記サーバ装置を攻撃対象とするコンピュータウイルスの発生の可能性を示す特異データを収集する収集ステップと、前記収集ステップにおいて収集された特異データに基づいて、前記コンピュータウイルスの発生の有無を判定するコンピュータウイルス発生判定ステップと、前記コンピュータウイルス発生判定ステップにおいて判定されたコンピュータウイルスの発生を前記セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムに通知する通知ステップと、をコンピュータに実行させるコンピュータウイルス発生検出プログラムである。

【0014】

【発明の実施の形態】以下、図面を参照しながら本発明の実施形態を説明する。

【0015】(第1実施形態) 図1は、本発明の第1実施形態に係るコンピュータウイルス発生検出装置の概略構成を示すブロック図である。図1に示すように、インターネット1に対して本発明に係るコンピュータウイルス発生検出装置3が接続されている。また、WWWサーバ5はファイアウォール4を介してインターネット1に接続されており、社内インターネット2はファイアウォール6を介してインターネット1に接続されている。ファイアウォール4及び6は、ともに不正なパケットをフィルタリング等するものであり、セキュリティ保護の観

点から設けられているが、本発明に必須の構成要素ではない。また図から明らかなようにWWWサーバ5はファイアウォール6を介して社内インターネット2の外側、すなわちインターネット1側に設けられている。このWWWサーバ5は、同サーバ5に対してなされたアクセスの経過記録(ログ)を保存するアクセスログ保存部8と、このアクセスログ保存部8に保存されているログを参照し、同サーバ5へのアクセスに関して発生したエラーを検出するエラー検出部7を備えている。

【0016】コンピュータウイルス発生検出装置3は、インターネット1上におけるコンピュータウイルスの発生の可能性を示す特異データを収集する手段として、例外ポート通信検出部31、不完パケット検出部32、通信量測定部33、およびエラー量測定部36を備えている。また、これら検出部31、32及び測定部33、36から得られた特異データに基づいて、コンピュータウイルス発生の有無を総合的に判定するコンピュータウイルス発生判定部34と、該コンピュータウイルス発生判定部34による判定結果に基づく異常発生通知を外部に報知するための異常発生通知送信部35を備えている。この異常発生通知送信部35は、ネットワーク停止判定／司令部9と通信するよう構成されており、ネットワーク停止判定／司令部9は社内インターネット2に作用し、社内インターネット2のインターネット1への接続を遮断(ネットワーク停止)したりする。なお、異常発生通知送信部35を設ける構成とせざり、例えばネットワーク管理者に対して、コンピュータウイルス発生判定部34により得られた判定結果をディスプレイ等により表示出力するよう構成してもよい。

【0017】このようなコンピュータウイルス発生検出装置3は、各種コンピュータ上で動作するソフトウェアとして実現可能である。

【0018】本明細書でいう「コンピュータウイルス」とは、記憶媒体や通信媒体等を通じて伝達し得るプログラム、データ、或いはその組み合わせからなる電子的情報であって、その情報の受信者が通常想定しない内容または形式のものである。例えば、悪意をもって情報の受信者のコンピュータの動作を異常とする目的の情報が典型的であるが、必ずしも悪意が無くとも不本意に作成されたりまたは不本意な使用法をするなどして想定外のふるまいが起こるもの全てを含む。また、伝達形態や媒体に関して特に制約は無く、記憶媒体に存在したり、ファイルの共有や電子メールによる送信により伝達したり、通常「ワーム」と呼ばれるインターネットを介して増殖する形式のものなど、さまざまな形態が考えられる。また、伝達される個々の情報そのものは通常想定されるものであるが、その組み合わせや伝達の順番、速度等によって同様の効果を生じるものも全体としてコンピュータウイルスと呼ぶことにする。

【0019】本実施形態のコンピュータウイルス発生検

出装置3は、このようなコンピュータウイルスがインターネット1上に発生したか否かを、同コンピュータウイルスを不特定のまま早期に検出するのであり、すなわち、種別やその仕組み等が明らかとなってワクチン等の対策データが提供される以前の状態、つまり未知コンピュータウイルスの状態でその発生を検出する。かかる検出のために、コンピュータウイルスの発生の可能性を示す特異データを収集するよう構成されている。ここでいう特異データとは、通常は使用されない例外ポートを使用したTCP/IP通信が行われたこと、異常なTCP/IP通信が行われたことによる不完全なパケットの発生、通信量の異常な増加、エラー量の異常な増加等を示すデータである。

【0020】図2は本実施形態に係るコンピュータウイルス発生検出装置の概略動作を示すフローチャートである。

【0021】先ずステップS1においてコンピュータウイルス発生検出装置3のインターネット1への接続処理が行われる。インターネット1への接続ののち、エラー量の測定(ステップS2)、例外ポート通信の検出(ステップS3)、不完パケットの検出(ステップS4)、および通信量の測定(ステップS5)が行われる。なお、図2においては、ステップS2～S5の処理が並列に実行されるものとして示してあるが、これらを任意の順番で逐次に実行してもよい。

【0022】これらステップS2～S5の処理においてコンピュータウイルスの発生の可能性を示す特異データが収集され、コンピュータウイルス発生判定部34に送られる。ステップS6において、コンピュータウイルス発生判定部34は、ステップS2～S5のそれこれから得られた特異データを元に総合的な判定を行って、未知コンピュータウイルス発生の有無を判定する。ここでの処理は、例えば、測定されたエラー量や通信量を所定のしきい値と比較する処理や、統計学的な処理、ヒューリスティックな処理を含む。

【0023】次に、ステップS7に示すように、コンピュータウイルスが発生したものと判定された場合はステップS8に移行する。そうでない場合はステップS2～S5の処理に戻る。

【0024】ステップS8においては、未知コンピュータウイルスが発生した旨の異常発生通知を異常発生通知送信部35がネットワーク停止判定／司令部9に対して送信する。

【0025】ここで、ステップS2におけるエラー量測定に基づくコンピュータウイルス発生判定の流れを図3のフローチャート及び図4乃至図7を参照して説明する。

【0026】先ずコンピュータウイルス発生検出装置3のエラー量測定部36は、WWWサーバ5にアクセスする(ステップS11)。コンピュータウイルスが発生し

た時点では、未だ社内インターネット2は同コンピュータウイルスに感染していない。なぜなら、コンピュータウイルスのほとんどは社外インターネット2の外部(特に海外)から発生し、最初にます「.com」ドメインなど在処がはっきりわかっているWWWサーバ5が狙われる。その後に、じわじわと他のサーバにコンピュータウイルスが蔓延し、コンピュータウイルスに感染したWWWサーバ5にユーザがブラウザ等でアクセスすることにより社内インターネット2が感染するという感染経路となるからである。これをコンピュータウイルス防御の観点から見れば、コンピュータウイルスの発生を最先で発見できるのは最初に狙われるWWWサーバ5であるということができる。

【0027】エラー量測定部36は、WWWサーバ5のエラー検出部7を通じて、アクセスログ保存部8に保存されているアクセスログのうち、エラーが生じたログを要求する。そしてエラー量測定部36はエラー検出部7から取得したエラーログを解析する(ステップS13)。

【0028】図4に、通常のアクセスが行われた場合のアクセスログ40を一例として示す。また、図5は、タイプミスによるエラーが生じた場合のアクセスログ50を一例として示す。

【0029】これらは、ユーザがブラウザなどで「http://ホスト/cool/vmware/FAQ.html」というURLのWEBページにアクセスした場合のログである。図4に示す41の内容は正しいURLであるが、図5の51に示すようにユーザがタイプミスなどすると、当該WWWサーバ5においては、50のようなエラーログが記録されることになる。これは、当該WWWサーバ5においてエラーとして処理されるのであるが、特にコンピュータウイルスを疑う余地はない。

【0030】一方、図6は異質なアクセスが行われた場合のアクセスログの一例を示す図である。近頃問題となつた「Nimda」のようなコンピュータウイルスの場合、WWWサーバ5のセキュリティホールを狙って図6の60に示すような異質なアクセスがなされ、エラーログとして記録される。

【0031】これは、図6における61及び62からなる非常に長い文字列を含んだURLを送ることにより、任意のプログラム(文字列62)をスタックに積んで、これを管理者権限(root権限)で実行させることを目的としており、一般に「アタック(攻撃)」と呼ばれている。アタックは、人間によるコマンド入力操作により行われたり、或いはプログラムにより自動的に行われたりする。

【0032】図6のような長大なURLが指定されたアクセスは、ステップS14において異質なアクセスである旨判定される(ステップS14)。これは、URLの文字列長を検査することで容易に判定される。

【0033】図7は異質なアクセスが行われた場合のアクセスログの他の例を示す図である。これは、Windows(R)オペレーティングシステム上で「c:\windown\system32\cmd.exe」を起動し、任意のプログラムを実行しようと試みるものである(文字列71で示される部分)。これもエラーログ70として記録される。この種のエラーログ70は、一見して「アタックである」ことが判断できないと考えられるが、明らかにユーザのタイプミスとは区別可能である。

【0034】コンピュータウイルス発生時には、一時的に、図6或いは図7のようなエラーが急増する。そこでステップS15においては単位時間あたりのエラーの異常増をエラー量測定部36により測定し、かかる測定結果をコンピュータウイルス発生判定部34による判定処理に供する。

【0035】なお、図3においてはステップS14において異質なアクセスである旨判定された場合に速やかにステップS16におけるコンピュータウイルス発生有無の判定に移行しているが、ステップS16に移行する前にエラー量の異常増を判定してもよい。あるいは、図6及び図7に示したような異質なアクセスであるか否かを判定せず、単にエラーの異常増のみを判定することによっても検出能を得ることはできる。

【0036】コンピュータウイルス発生判定部34は、エラー量測定部36により測定されたエラーの異常増を示す特異データを元に、これを所定の閾値と比較するなどしてコンピュータウイルスの発生有無を判定する。なお、この場合の閾値を、ユーザが任意に設定変更できるようユーザインターフェースを設けることが好ましい。

【0037】コンピュータウイルス発生判定部34によりコンピュータウイルスが発生した旨の判定が下されると、この情報は異常発生通知送信部35に送られる。異常発生通知送信部35は、ネットワーク停止判定／司令部9との通信を確立し、コンピュータウイルス発生の旨を示す異常発生通知を送信する。この異常発生通知を受けたネットワーク停止判定／司令部9は、例えば図8に示すような切断位置でインターネット1との接続を遮断する。

【0038】このような本実施形態によれば、社内インターネット2からファイアウォール4、6を介した外側のインターネット1上において、コンピュータウイルスの発生をコンピュータウイルス発生検出装置3によって検出することができ、該コンピュータウイルスの発生を検出した時点で、社内インターネット2が未感染であることを十分に期待できるようになる。そして、当該コンピュータウイルスに関する詳細情報や対策情報が明らかとなるまでの期間、必要に応じて社内インターネット2を停止させたり、WWWなど一部のサービスを停止させることができようになる。特に、本実施形態によれば

既知のコンピュータウイルスのみならず未知のコンピュータウイルスをもその発生をほぼ完全に検出できるようになる。これは、セキュリティ対策上極めて効果的であり、コンピュータウイルス感染が蔓延して被害が急速に拡大する前に適切な対策を講じることができるようになる。具体的にいうと、コンピュータウイルスは米国時間の昼間に広がことが多いのであるが、日本時間の夜間、つまり従業員の出社前に対策を講じることができるようになる。

【0039】尚、未知コンピュータウイルスの発生が検出された場合、これが危険なコンピュータウイルスであるか否かについて最終的に人間が判断を下すよう構成することが好ましい。これは、コンピュータウイルス発生判定部34や異常発生通知送信部35がシステム管理者等の操作介入を受け付けるよう構成することで実現できる。一方、このような人間による判断を行わず、ネットワーク停止判定／司令部9が自動的にネットワークの停止を行うことは、社内インターネット2の運用上、支障を来すこととも考えられるが、それでも、攻撃にさらされたままにするよりは良いと考えられる。特に、夜間は無条件に社内インターネット2を停止させることができない。

【0040】(第2実施形態) 上記第1実施形態は、コンピュータウイルス発生検出装置3を、ファイアウォール6を介して社内インターネット2の外側に設けるものであった。一方、本発明の第2実施形態は、コンピュータウイルス発生検出装置3を社内インターネット2の内部に設ける構成としたものである。図9はこのような本発明の第2実施形態を示す概略構成図である。

【0041】コンピュータウイルス発生検出装置3の内部構成は、上記第1実施形態にて説明したものとほぼ同様であるが、本実施形態の場合、アタック検出の対象とするサーバをWWWサーバ5ではなく、図示しない社内インターネット2内部のサーバとすることができます。このほか、例外ポート通信検出、不完パケット検出、通信量測定についても、社内インターネット2内を検出又は測定対象とすることができる。このような第2実施形態の場合、社内におけるコンピュータウイルス被害への対策を第1実施形態と同様に早期に行うことができるようになる。また、コンピュータウイルスの発生が社内インターネット2の外部からのものであることが判明した場合、図9に示すように外部との接続を遮断することもできるようになる。

【0042】また、本実施形態においては、コンピュータウイルス発生検出装置3と協働する駆除対策部80が設けられている。この駆除対策部80は、既知コンピュータウイルスを駆除するための対策データとして、例えばパターンファイルやセキュリティホールを手当する修正プログラム等を社内インターネット2内のクライアントマシンに配布するものである。なお、このような駆除

11

対策部 80 は、上記第 1 実施形態の構成に付加されてもよいことは勿論である。

【0043】このような本発明の第2実施形態によっても第1実施形態と同様の作用効果を得ることができる。なお、アタック検出の対象とするサーバを、社内のもののみならず、社外のサーバ（例えばWWWサーバ5）を含め複数台とすれば、コンピュータウイルスの検出性能をさらに高めることができるようになる。

【0044】なお、本発明は上述した実施形態に限定されず種々変形して実施可能である。例えば、ファイル感染型、マクロ感染等の既知コンピュータウイルスの検出及び対策を本発明の実施と併用することで、セキュリティ対策をより強固なものとすることが好ましい。

[0045]

【発明の効果】以上説明したように、本発明によれば、ネットワーク上でのコンピュータウイルスの発生を早期に検出し、セキュリティ保護の対象となるコンピュータネットワーク又はコンピュータシステムへのコンピュータウイルスの感染被害を未然に防止できるコンピュータウイルス発生検出装置、方法、およびプログラムを提供できる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係るコンピュータウイルス発生検出装置の概略構成を示すブロック図。

【図2】上記実施形態に係るコンピュータウイルス発生検出装置の概略動作を示すフローチャート

【図3】上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定の流れを示すフローチャート

【図4】上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定を説明するための図であつて、通常のアクセスが行われた場合のアクセスログの一例を示す図

10

【図5】上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定を説明するための図であつて、タイプミスによるエラーが生じた場合のアクセログの一例を示す図

【図6】上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定を説明するための図であつて、異質なアクセスが行われた場合のアクセスログの一例を示す図

【図7】 上記実施形態に係るエラー量測定に基づくコンピュータウイルス発生判定を説明するための図であって、異質なアクセスが行われた場合のアクセスログの一例を示す図

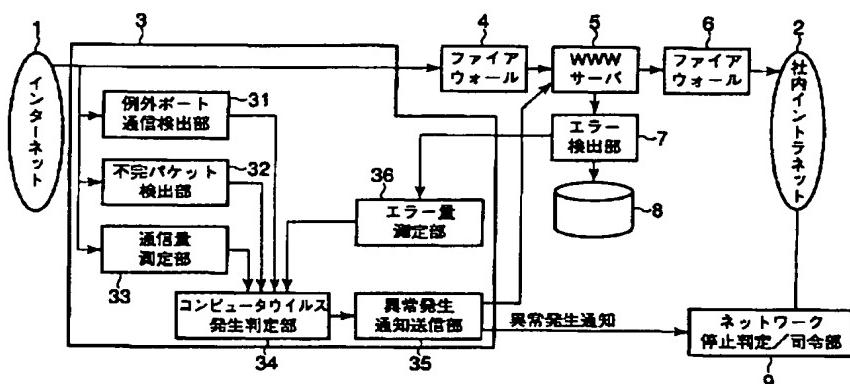
【図8】 上記実施形態に係るコンピュータウイルス発生時における対策処理を説明するための図であって、ネットワークの切断位置を示す図

【図9】 本発明の第2実施形態に係る概略構成図

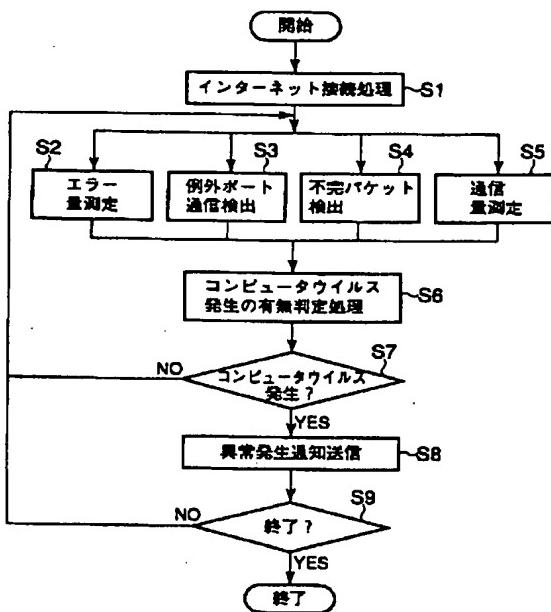
【符号の説明】

- 1 …インターネット
 - 2 …社内イントラネット
 - 3 …コンピュータウイルス発生検出装置
 - 4, 6 …ファイアウォール
 - 5 …WWWサーバ
 - 7 …エラー検出部
 - 8 …アクセスログ保存部
 - 9 …ネットワーク停止判定／司令部
 - 3 1 …例外ポート通信検出部
 - 3 2 …不完パケット検出部
 - 3 3 …通信量測定部
 - 3 4 …コンピュータウイルス発生判定部
 - 3 5 …異常発生通知送信部
 - 3 6 …エラー量測定部

[图11]



[図2]



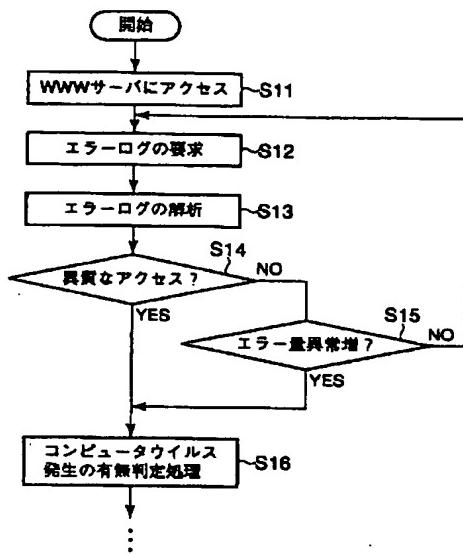
[図4]

2001/12/26 15:05:43 JST 32.97.110.70 ss05. co. us. ibm. com-
GET /coal/vmware/FAQ..html HTTP/1.0 200
41 7
40

[図 6]

[図 8]

[图3]

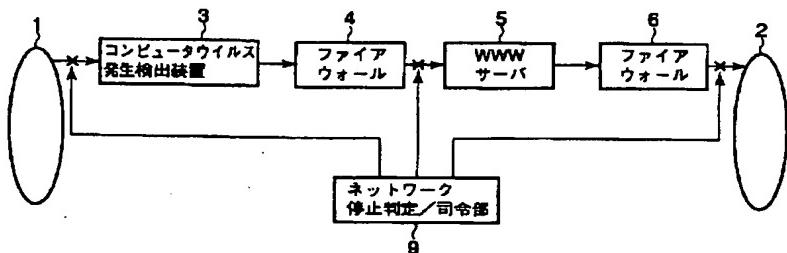


[図 5]

2001/12/28 13:35:49 JST 207.140.168.143 crawler. tlvra.com
GET /cool/vmware/FAQ.html HTTP/1.0 404 "File Not Found"
51 50

【图 7】

2001/09/18 22:17:51 JST 210.232.186.38 www2.tomonet.co.jp-GET [/c/winnt/system32/cmd..exe ?/c+dir HTTP/1.0 404 -70 "File Not Found" -71



【図9】

